National Institute of Standards and Technology
U.S. Department of Commerce

# *Cyber SCRM Update to NIST Cybersecurity Framework 1.1*

IT Laboratory
NIST

*Software and Supply Chain Assurance Forum*

*5 October 2016*

## *"Roadmap for Improving Critical Infrastructure Cybersecurity: Areas for Development, Alignment, and Collaboration"* February 2014

- The Executive Order calls for the framework to "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations"
- The Roadmap, based on stakeholder input, identified supply chain risk management as an area for future focus:
  - Authentication
  - Automated Indicator Sharing
  - Conformity Assessment
  - Cybersecurity Workforce
  - Data Analytics
  - Federal Agency Cybersecurity Alignment
  - International Aspects, Impacts, and Alignment
  - Supply Chain Risk Management
  - Technical Privacy Standards

# Framework Core

*Cybersecurity Framework Component*

| Function | Category | ID |
|---|---|---|
| **Identify** | Asset Management | **ID.AM** |
| | Business Environment | **ID.BE** |
| | Governance | **ID.GV** |
| | Risk Assessment | **ID.RA** |
| | Risk Management Strategy | **ID.RM** |
| **Protect** | Access Control | **PR.AC** |
| | Awareness and Training | **PR.AT** |
| | Data Security | **PR.DS** |
| | Information Protection Processes & Procedures | **PR.IP** |
| | Maintenance | **PR.MA** |
| | Protective Technology | **PR.PT** |
| **Detect** | Anomalies and Events | **DE.AE** |
| | Security Continuous Monitoring | **DE.CM** |
| | Detection Processes | **DE.DP** |
| **Respond** | Response Planning | **RS.RP** |
| | Communications | **RS.CO** |
| | Analysis | **RS.AN** |
| | Mitigation | **RS.MI** |
| | Improvements | **RS.IM** |
| Recover | Recovery Planning | **RC.RP** |
| | Improvements | **RC.IM** |
| | Communications | **RC.CO** |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2<br>NIST SP 800-53 Rev. 4 CP-2, SA-12 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | COBIT 5 APO02.06, APO03.01<br>NIST SP 800-53 Rev. 4 PM-8 |
| **ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated | COBIT 5 APO02.01, APO02.06, APO03.01<br>ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6<br>NIST SP 800-53 Rev. 4 PM-11, SA-14 |
| **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3<br>NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5**: Resilience requirements to support delivery of critical services are established | COBIT 5 DSS04.02<br>ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 |

ds and Technol

# Goals

- Update Gaps (What we heard)
- Minimal to no disruption – backwards compatible
- Minimize document “bloat”

# Gaps – what is NOT in the Framework

| | |
|---|---|
| **Identifying and Categorizing Suppliers** | **ISO/IEC 27036 2; 6.2.3: Define, implement, maintain and improve a process for identifying and categorizing suppliers or acquirers…..** |
| **Monitoring and Improvement** | **ISO/IEC 27001: 9 Performance evaluation; 9.1 Monitoring, measurement, analysis, and evaluation; 9.2 Internal audit; 9.3 Management Review<br>ISO/IEC 27001: 10 Improvement ; 10.1 Nonconformity and corrective action; 10.2 Continual Improvement** |
| **Risk Monitoring** | **SP 800 161 TASK 4 2: Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.** |
| **Hardware Assurance** | **Multiple information security standards, e.g. SAE standards; as well as cyber supply chain standards/guidelines, such as SP 800 161, ISO/IEC 27036 and 20243 (O TTPS).** |

# 2015/16 RFI Responses on Supply Chain

## Major concern of respondents

- Gaps
  - Framework does not recognize the interdependencies of sectors based on their supply chains
  - The Framework doesn't supply method of reducing third party risk
  - Framework should take a lifecycle approach to supply chain management
  - Does not address tainted/counterfeit products
- Recommendations
  - Unique supply chain overlays
  - Add high-level SCRM text to broader body of the Framework
  - Expand Informative References
  - Focus on international supply chain security

# Current Thinking on Areas to Update

- 3.3 Communicating Cybersecurity Requirements with Stakeholders
  - Expand Subsection 3.3 to more explicitly reference SCRM importance, methodology, and vocabulary
- Framework Implementation Tiers
  - Partial/Risk Informed/Repeatable/Adaptive
    - Risk Management Process, Risk Management Program, External Participation
- Framework Core

# Framework Core - Identify

| | |
|---|---|
| **Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks. | **ID.SC-1:** Supply chain risk management processes are identified, established, managed, and agreed to by organizational stakeholders. |
| | **ID.SC-2:** Critical suppliers/providers are identified and supply chain risk assessments are conducted as a part of the supplier/provider selection process. |
| | **ID.SC-3:** Suppliers/providers are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Supply Chain Risk Management Plan. |
| | **ID.SC-4:** Suppliers/providers are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of your suppliers/providers are conducted. |

# Framework Core - Protect

| | |
|---|---|
| **Data Security (PR.DS)**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information | **PR.DS-1:** Data-at-rest is protected |
| | **PR.DS-2:** Data-in-transit is protected |
| | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition |
| | **PR.DS-4:** Adequate capacity to ensure availability is maintained |
| | **PR.DS-5:** Protections against data leaks are implemented |
| | **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity |
| | **PR.DS-7:** The development and testing environment(s) are separate from the production environment |
| | **PR.DS-8**: Integrity checking mechanisms are used to verify hardware integrity. |


**Jon Boyens**
Program Manager
ICT SCRM
NIST
Jon.Boyens@nist.gov

Http://scrm.nist.gov